29.3.4. Чување, заштита и сигурност података у информационом систему еЗУП.

Надлежни орган одговоран је за чување, заштиту и сигурност података у оквиру информационог система еЗУП, што нарочито подразумева:

1) заштиту од неовлашћеног приступа ресурсима који су предмет заштите, њихово неовлашћено коришћење или манипулације базом података информационог система од стране интерних и екстерних корисника;

2) заштиту интегритета података, њихову расположивост и неовлашћени увид у поверљиве податке;

3) заштиту информационог система еЗУП од злонамерних софтвера;

4) осигурање преноса података кроз информациони систем еЗУП интерним и екстерним корисницима;

5) чување података и управљање сигурносним копијама базе података у оквиру информационог система;

6) осигурање континуитета активности у случају пожара, поплаве, земљотреса или друге непогоде која се сматра резултатом више силе и која доводи до неуобичајеног прекида у раду информационог система;

7) повраћај сачуваних података у случају губитка, оштећења или уништења рачунарске опреме информационог система;

8) инсталирање софтверске надоградње ради уклањања сигурносних проблема који се установе у информационом систему или на повезаном софтверу;

9) праћење сигурносних инцидената у информационом систему ради предузимања корективних мера;

10) управљање сигурносним инцидентима, едукација и обука свих овлашћених особа ради стицања потребних знања о чувању и сигурности података;

11) физички приступ и заштита базе података у оквиру информационог система и рачунарске опреме;

12) одржавање рачунарске опреме информационог система;

13) примену и других мера заштите предвиђене Актом о безбедности ИКТ система од посебног значаја, као и прописима о информационој безбедности.

Орган који води службену евиденцију из које се прибављају и достављају подаци преко информационог система еЗУП одговоран је за чување, заштиту и сигурност података из своје службене евиденције.

29.3.5. Мере заштите приступа информационом систему еЗУП.

Мере заштите приступа информационом систему еЗУП јесу:

1) аутентикација – која представља процес утврђивања идентитета особе која жели да приступи информационом систему еЗУП;

2) ауторизација – која представља право приступа и дозвољених операција за аутентиковано лице;

3) заштита тајности – што подразумева шифровање података у циљу спречавања неовлашћеног увида;

4) непорицање одговорности – што подразумева обезбеђење доказа да је неко извршио одређену радњу, односно трансакцију.

Реализација система заштите информационог система еЗУП подразумева обавезну примену квалификованих електронских сертификата за приступ информационом систему еЗУП и аутентикацију трансакција, као и за аутентикацију приступа веб-сервисима. Поред тога, аутентикација приступа сервисима од стране органа који преко информационог система еЗУП врше размену података подразумева и обавезну примену серверских сертификата.

29.3.6. Приступ информационом систему еЗУП.

Надлежни орган управља корисничким налозима, правима приступа и корисничким лозинкама за кориснике информационог система еЗУП, а дужан је да